Trajnimi për Auditimin e Avancuar të Active Directory (AD) dhe IT Financial Audit me ekspertët norvegjezë në datat 28 tetor – 1 nëntor

Në kuadër të marrëveshjes dypalëshe të bashkëpunimit me SAI-n e Norvegjisë, u zhvillua në KLSH në datat 28 tetor – 1 nëntor 2024, trajnimi i radhës me ekspertët norvegjezë për auditimet IT. Qëllimi kryesor i trajniit të radhës ishte përmirësimi i cilësisë së auditimeve të IT-së në KLSH, me fokus në Sigurinë e Informacionit dhe Qeverisjen e IT-së.

Tematikat e trajtuara gjatë trajnimit janë si vijon:

Auditimi i Avancuar i Windows dhe Active Directory (AD):
- Kuptimi i parimeve të rrjeteve Windows dhe AD Domain System;
- Identifikimi i rreziqeve të avancuara të sigurisë në AD Domain System, Serverat Windows dhe përdoruesit e windows;
- Përdorimi i programit të auditimit dhe CIS Benchmark për auditimin e rrjeteve Windows dhe AD;
- Inkorporimi i gjetjeve në një raport të gjerë të sigurisë së informacionit.

Auditimi i IT në Sistemet Financiare:
- Kuptimi i kërkesave për auditimin e sistemeve të informacionit financiar;
- Praktikimi i auditimit financiar sipas ISSAI 2315 për sistemet financiare të KLSH-ës.

Trajnimi kontribuon në përmirësimin e kapaciteteve të auditimit të IT-së, por siguron edhe që audituesit e KLSH-së, të jenë të pajisur me aftësitë dhe mjetet e nevojshme për t'u përshtatur me kërkesat në zhvillim të auditimit të IT-së, duke forcuar kështu efektivitetin dhe thellësinë e praktikave në auditim.

Angazhimi i KLSH për zhvillimin e njohurive në auditime e Sigurisë Kibernetike dhe Financiare të IT-së mbetet një objektiv afatgjatë, i fokusuar në sigurimin e trajnimeve të vazhdueshme dhe përmirësimin e metodologjive të auditimit.

Me bashkëpunimin e vazhdueshëm me SAI e Norvegjisë për vitin 2025 janë planifikuar të realizohen 3 tema të tjera, të cilat janë po me aq interes sa ato që janë zhvilluar deri tani, për institucionin dhe për audituesit e Teknologjisë së Informacionit.

I. **Testime penetrimi në Infrastrukturën e IT.**

Testimi i penetrimit (pen testing) në infrastrukturën e IT është një proces kyç për vlerësimin e sigurisë së sistemeve dhe rrjeteve të teknologjisë së informacionit. Ky testim synon të identifikojë dobësitë dhe mundësitë që mund të shfrytëzohen nga një sulmues.

Procesi përfshin disa hapa kryesorë:

- Skantimi i Rrjetit dhe Vulnerabiliteteve, për të gjetur dobësitë e mundshme të sigurisë.
- Përdorimi i mjeteve automatike për identifikimin e dobësive.
- Shfrytëzimi i dobësive të zbuluara për të hyrë në sistemet dhe për të simuluar një sulm të mundshëm.

Në përfundim të testimit, do të hartohet një raport i detajuar që do tw jetw një udhëzues për menaxhimin e IT-së për të adresuar çështjet dhe për të forcuar mbrojtjen, ku do tw përfshihen:

- Një përshkrim të dobësive të identifikuara.
- Metodat që janë përdorur për të shfrytëzuar dobësitë.
- Propozime për përmirësimin e sigurisë dhe eliminimin e dobësive.

Testimi i penetrimit është një pjesë thelbësore e auditimeve të sigurisë IT dhe duhet të kryhet rregullisht për të siguruar që infrastruktura mbetet e mbrojtur nga kërcënimet e mundshme.

II. **Sulme Phishing**

Një nga temat më të nevojshme sot në cdo institucion dhe që nuk përqëndrohet vetëm në IT por në të gjithsë struktrurën pasi sulmet phishing ofrojnë disa përfitime të rëndësishme për institucionet që duan të përmirësojnë sigurinë e tyre kibernetike:

- Testimet e phishing ndihmojnë stafin të njohë taktikat e sulmeve dhe të identifikojë email-e të dyshimta. Me trajnim dhe përvojë praktike, punonjësit bëhen më të vetëdijshëm për rreziqet dhe për mënyrën si të shmangin klikimet e rrezikshme.
- Testet identifikojnë dobësitë dhe pikat e dobëta, sidomos ato që lidhen me ndërveprimin e punonjësve me sistemet e email-eve dhe internetin.
- Duke testuar dhe analizuar reagimin e stafit ndaj një sulmi phishing, instiutcionet mund të përmirësojnë protokollet e tyre të reagimit ndaj incidenteve kibernetike. Kjo është thelbësore për të siguruar që në rastin e një sulmi të vërtetë, të ketë reagim të shpejtë dhe efikas.
- Ndërgjegjësimi dhe trajnimi ndihmojnë në zvogëlimin e shanseve që një sulm phishing të ketë sukses. Sa më të përgatitur të jenë punonjësit për të njohur dhe shmangur këto sulme, aq më i ulët është rreziku për insttiucionin.

III. **Auditimi i faqeve Web dhe Aplikacioneve Web.**

Ky auditim është i rëndësishëm për të siguruar që sistemet online të jenë të mbrojtura nga cenimet kibernetike dhe të përmbushin standardet e sigurisë. Ky proces synon të rrisë sigurinë e faqeve web dhe aplikacioneve, duke garantuar që përdoruesit dhe të dhënat e tyre të jenë të mbrojtura nga kërcënimet kibernetike.

Audituesit që morën pjesë aktive në këtë trajnim, përdorën e testuan mjete të teknologjisë që SAI i Norvegjisë disponon për auditimet që kryen në këtë drejtim. Pjesëmarrës ishin: Elira Cukalla, Rodjan Alimerkaj, Klea Saliu, Ardit Alushaj, Anxhela Kostaj, Megi Peza, Arjola Mucaj, Rovenda Deda dhe Xhesika Nano